Full functionality of this form requires Adobe Acrobat Reader 4.0 or above.

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

Download Reader 4.0

PRIVACY ACT STATEMENT

Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)." Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set for at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 551a(b) of the Privacy Act

TYPE OF REQUEST	DATE
☐ INITIAL ☐ MODIFICATION ☐ DELETION	03-Mar-2003

PART I *(To be completed by User)*

1. NAME (Last, First, MI)		2. SOCIAL SECURITY NUMBER (Last 4) Not Applicable
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. ACCOUNT CODE Not Applicable
6, JOB TITLE/FUNCTION	7. GRADE/RANK	8. PHONE (DSN)

STATEMENT OF ACCOUNTABILITY: I understand my obligation to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized access.

USER SIGNATURE	DATE

PART II *(To be completed by User's Security Manager)*

9. CLEARANCE LEVEL Not Applicable	10. TYPE OF INVESTIGATION Not Applicable	11. DATE OF INVESTIGATION
12. VERIFIED BY (Signature) Not Applicable	13. PHONE NUMBER Not Applicable	14. DATE Not Applicable

PART III *(To be completed by User's Supervisor)*

15. ACCESS REQUIRED *(Location - i.e., FTEMP, etc.)*

16. ACCESS TO CLASSIFIED REQUIRED?	17. TYPE OF USER	
☒ NO ☐ YES	☒ FUNCTIONAL ☐ SYSTEM	☐ SECURITY ADMINISTRATOR ☐ APPLICATION DEVELOPER ☒ OTHER (Specify)

18. JUSTIFICATION FOR ACCESS

VERIFICATION OF NEED TO KNOW

I certify that this user requires access as requested in the performance of his/her job function.

19. SIGNATURE OF SUPERVISOR	20. ORG/DEPT	21. PHONE NUMBER (DSN)	DATE
23. PRINTED NAME/SIGNATURE OF DATA OWNER/OPR	24. ORG/DEPT	25. PHONE NUMBER	DATE

PART IV *(To be completed by AIS Security Staff adding user)*

27. USERID (Mainframe)	28. USERID (Mid-Tier)	29. USERID (Network)	
30. SIGNATURE		31. PHONE NUMBER	DATE

Next Page

Section 33c Instructions

PART V ***(Can be customized by DISA or Customer with DISA approval (Optional))***
(To be completed by User)

33. OPTIONAL USE (MODIFIED FOR AFFTC-MIS SYSTEMS, EDWARDS AFB, CALIFORNIA)

a. E-MAIL ADDRESS

b. WORK MAILING ADDRESS (Include building number and room number)

c. PROJECTS FOR WHICH ACCESS IS REQUIRED (Refer to the instruction page for information)

PROJECTS (APPLICATIONS)	JOB FUNCTION (REQUIRED ACCESS)	APPROVAL SOURCE/SIGNATURE	DATE
Edwards Home Page	Intranet Site Adminis		

MIS SERVICES USE ONLY

34. APPROVED BY/ DATE	35. ENTERED INTO THE DATABASE BY/DATE	
36. ORACLE/SQL NAME	37. ROLES ASSIGNED	
38. USERNAME	39. UIC (IF APPLICABLE)	40. USER_ID

41. REMARKS

Reset Form Print Form

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER_ID.

TYPE OF REQUEST: INITIAL for a first time submission. MODIFICATION for any changes to existing account. DELETION to delete an existing account.
(1) NAME: The last name, first name and middle initial of the user.
(2) SOCIAL SECURITY NUMBER: The social security number of user. (Not Required)
(3) ORGANIZATION: The user's current organization (e.g., 412 TW).
(4) OFFICE SYMBOL/DEPARTMENT: The office symbol within the current organization (e.g., RMSS).
(5) ACCOUNT CODE: Account code, if required. (Not Required)
(6) JOB TITLE/FUNCTION: The job function (e.g., System Analyst, Pay Clerk, etc.).
(7) GRADE/RANK: The civilian pay grade, military rank with component, or CONT with company name, if user is a contractor.
(8) PHONE (DSN): The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
USER'S SIGNATURE: User must sign the SAAR form with the understanding that he/she is responsible and accountable for the assigned password and access to the system(s).

B. PART II: The following information is provided by the User's Security Manager. (Not Required)

(9) CLEARANCE LEVEL: The user's current security level and ADP Level (e.g., Secret, Top Secret, etc.).
(10) TYPE OF INVESTIGATION: The user's last type of background investigation (e.g., NAC, NACI, or SSBI).
(11) DATE OF INVESTIGATION: The date of the last background investigation.
(12) SIGNATURE: The Security Manager or his/her representative's signature indicates that the above clearance and investigation information has been verified.
(13) PHONE NUMBER: The Security Manager's phone number.
(14) DATE: The date that the form was signed by the security manager or his/her representative.

C. PART III: The following information is provided by the user's supervisor.

(15) ACCESS REQUIRED (Location): The full name of the location at which access is required.
(16) ACCESS TO CLASSIFIED REQUIRED?: Place an "X" in the "NO" box.
(17) TYPE OF USER: Place an "X" in the FUNCTIONAL box, unless you are a part of the RMS System Support Team
(18) JUSTIFICATION FOR ACCESS: A brief statement to justify establishment of an initial USERID.
Provide appropriate information if the USERID or access to the current USERID is to be modified.
(19) SIGNATURE OF SUPERVISOR: The user's supervisor must sign the SAAR form to certify the user is authorized access to perform his/her job function.
(20) ORG/DEPT.: Supervisor's organization and department.
(21) PHONE NUMBER: Supervisor's phone number.
(22) DATE: The date the supervisor signs the SAAR form.
(23) PRINTED NAME/SIGNATURE OF DATA OWNER/OPR: Signature of the functional appointee responsible for approving access to the system being requested.
(24) ORG./DEPT.: Functional appointee's organization and department.
(25) PHONE NUMBER: Functional appointee's phone number.
(26) DATE: The date the Functional appointee signs the SAAR form.

D. PART IV: The following information is provided by the RMS System Security Staff who adds the user to the system.

(27) USERID (Mainframe): User's mainframe USERID (if applicable)
(28) USERID (Mid-Tier): User's mid-tier USERID (if applicable)
(29) USERID (Network): User's network USERID (if applicable)
(30) SIGNATURE: Signature of the RMS System Administrator or his/her representative
(31) PHONE NUMBER (DSN): The Defense Switching Network (DSN) phone number
(32) DATE: The date the system administrator signs the SAAR form

E. PART V; This information is site specific and can be customized by either the DMC, functional activity, or the customer with approval of the DMC. This information will specifically identify the access required by the user.

(33) OPTIONAL USE: This section is intended to add site specific information, as required.

INSTRUCTIONS FOR FILLING IN PART V OF THE FORM

33. OPTIONAL USE
a. E-MAIL ADDRESS: Work E-mail address (if available) so any necessary information can be sent to the user.
b. WORK MAILING ADDRESS: The postal mailing address of the user's work place. Please include all pertinent information, e.g., address, street, bldg, room, suite, city, state, zip code. This is necessary in case the form needs to be mailed back to the requesting user for some reason. Include the building number and room number for remote printer requirements.
c. PROJECTS FOR WHICH ACCESS IS REQUIRED (Enter all required access).
PROJECTS - Enter the name of the projects or applications that you want access to the MIS systems.
JOB FUNCTION - Enter the access level, role or access type for a particular project or projects. A project may have several job functions.
APPROVAL SOURCE/SIGNATURE - This is an MIS function column. MIS personnel will ensure you have a need to access the particular project(s) and you are allowed to perform the requested access.
DATE - This is the date the MIS personnel signed the requested access.

Below is the sample list of projects and job functions that can be selected:

ABSS JOB FUNCTIONS:
BASIC USER - Drafts and submits new financial documents
RESOURCE ADVISOR - Verifies financial information and approved financial documents
APPROVER - Financial manager who approved funds
MODULE MANAGER - Maintains agency specific information including organizational form flow, accounting codes
CERTIFYING OFFICER - Certifies financial documents
ACCEPTING OFFICER - Budget function
CONTRACTING OFFICER - BCAS interface
OPLOC USER - DFAS personnel
OTHER - Other access required

Reset Form Print Form

INSTRUCTIONS FOR FILLING IN PART V OF THE FORM (continued)

CENTER - MIS JOB FUNCTIONS:

BUDGET ANALYST (BA) - Responsible for managing project funds, validates the reimbursement code for the Project, validates project work phases according to the official work phase matrix, and approves Project funding status.
COST SERVICE (CS) - Responsible for the creation and publication of product and service structure and costs/rates. Develops the indirect and overhead rates and local assessments for the product and service structure.
COST ANALYST (CA) - Responsible for reviewing the resources and costs for a project and assigns the Test Program Cost Estimate and Cost Annex for all estimates.
PROGRAM ANALYST (PA) - Responsible for generating the statement of capability, validates the Project work phases according to the official work phase matrix, and approves Project concurrence.
RESPONSIBLE PROGRAMS OFFICER (RPO) - Creates the new JON and assigns the project positions. Establishes the initial work phase according to the official work phase matrix, and approves Project concurrence.
PROJECT VIEW (PV) - Allows the user access to Project for viewing purposes only, cannot update.
REPORTS - Job function requires access to Center-MIS reports for viewing and printing capability (e.g., JOR, PMR, TSP, TPCEA, Cost Data, Product Service Reports, and Flying Hour Data Reports).
WORKLOAD FORECAST ESTIMATOR - Enters flying hour projections for the Workload Forecast process.
WORKLOAD FORECAST APPROVER - Approves estimates for the Workload Forecast process.
SPECIAL PROJECT TASKS/PRIVILEGES (Each has two levels of privileges to be approved).

BUDGET ANALYST APPOINTER:	Assigns another BA to a specific Project or to all Projects
COST ANALYST APPOINTER:	Assigns another CA to a specific Project or to all Projects
PROGRAM ANALYST APPOINTER:	Assigns another PA to a specific Project or to all Projects
REIMBURSEMENT CODE:	Assigns RC to Project or to all Projects
PROJECT FUNDING STATUS:	BA that approves activation of Project in coordination with PA/RP concurrence/ approval

OTHER - Other functions

ESS/781 JOB FUNCTIONS:

ESS GROUPS:

CENTER SCHEDULING - Scheduling, Data Reporting, Real time flight coordination
CTF - Scheduling, Data Reporting, Crew Entry, and Authorization (AF Form 83)
ESS_ADMIN - Administration
READONLY - Data Reporting and Viewing
OTHER - Any other

781 GROUPS:

ARGJOC - ARGUS or JOCAS Usage
DEVEL_GROUP - Administration
OSCR_GROUP - Flight Records Personnel
PILOT_GROUP - Pilot Usage
READONLY - Data Reporting and Viewing
OPS_GROUPO - CTF Operations Desks
PM_GROUP - JON or Program Manager Usage
OTHER_GROUP - Any other

JOCAS JOB FUNCTIONS

AD HOC REPORTS - Generates Reports using IQ
ASSET MANAGER - View and Enter Capital Assets
CAO - Cost Accounting Office users
CCAO - Chief of the Cost Accounting Office
COST ENTRY - View and Enters Costs transactions
CUSTOMER FOCAL - Views, enters and approves Labor transactions
FDBA - Functional Database Administrator
JON ESTIMATE - Views and enters JON estimates
JON MANAGER - Views, enters and updates JON information
LABOR ENTRY - Views and enters labor transacctions
PS ENTRY - Views and enters product and service transactions
MAINT - JOCAS maintenance
PS_APRV - Views, enters and approves product and service transactions
RON_MANAGER - Views, enters and updates RON information
STDREPORTS - Generates and Schedules standard reports
SQLPLUS - Access to the database
SUPERVISOR - Managerial position that approves labor transactions

WINFRAME ACCESS (Application Server):

WEB/NT ACCESS:

WEB SITE (FRONT PAGE) - Access to the front page:
DEVELOPER
ADMINISTRATOR
AUTHOR
APPROVAL AUTHORITY
WEB SITE ACCESS - Access to parent/child WEB SITES
NT USER -Access to drive/folder mapping
OTHER - Other type of access

OTHERS: (Other access not specified above)

F. DISPOSITION OF FORM

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be handled as such.
FILING: Original SAAR, with original signatures in Parts I, II, and III must be maintained on file for 1 year after termination of user's account. File may be maintained by the system's Security Officer. Recommend file be maintained by adding the user to the system.

Reset Form Print Form